GRAPHICAL PASSWORD AUTHENTICATION USING CaRP

Ragavendra .A, Jeysree .J

Abstract—The security initiative work is very vital one in all computing features enabled platform, the work of this project states about implementation of Graphical Password Authentication using CaRP (Captcha as gRaphical Passwords).This new security primitive is based on hard AI problems. It is built on both texts based Captcha and image-recognition based Captcha. Here the images used in CaRP are distorted format as like Captcha challenges. It's a kind of authentication response test. It addresses the various security based attacks. It ensures the users with secured login authentication. It fit well with the some practical applications.

Keywords: CaRP, click based authentication, Graphical password, recognition based validation, Hash visualization, usable security.

I. INTRODUCTION

Security is important factor in today's world. It is essential for accessing confidential data and security parameters were done based on the cryptography and mathematical calculation. In this paper its state about two level of authentication method which is different from existing techniques. Cryptography is based on the many encryption and decryption algorithms. Here this paper come up with hash table values by salt method.AI (artificial intelligence) used to create a hard security challenges. It uses the captcha techniques to provide the security on user interface. Captcha's given as Completely Automated Public Turing test to tell computers and Humans Apart. It's mainly used for users to accessing their protected resources. It is a kind of challenge response test use to compute specifically whether the user is human or not. The essential and underlying task in this security based project is to create secured login authentication towards the end user with the help of cryptographic technique named MD5 hash algorithm, security primitives based on hard AI mathematical problems that are computationally intractable with humans like existing captcha. Comparatively hard to computer bots, malwares and online guessing attacks. In this project both click text based captcha grid and click image based captcha grid plays a vital role to ensure the security for end user validation.

II. PROBLEM STATEMENT

The problems of knowledge-based authentication are extremely text-based passwords are well known. Users often needs to create memorable passwords that are easy for attackers to guess, but Strong system-assigned passwords are difficult for users to remember, a graphical password authentication system should encourage users with strong passwords as well as memorable. So they came through with new ideas like

->recognition based (pass faces),

->recall based (Das),

->persuasion using cued click points (pass points).

In the area of graphical passwords, Recognition based (pass faces) having high level of online guessing attacks. Recall based (draw a secret) shows high password strength but it needs very low level of attempts to crack the password. Cued click points is the latest technique which gives hot spot images(i.e.)highlighting the points to the attackers. This paper overcomes the above issue with following authentication ideas incorporate with graphical password techniques.

III. RELATED WORKS

A ***recognition-based*** method requires identifying among steerer the visual objects belonging to a password portfolio. A typical idea is Pass faces wherein a user selects a portfolio of faces from a database which creating a password. During the time of authentication, a panel of nominee faces is presented for the user to select the face belonging to their portfolio. This process is continual several rounds, each round with a dissimilar group panel. A triumphant login requires correct selection in each round. The set of images in a panel remains the distinct between different logins, but their locations are changed and a user must identify their respective portfolio images in the exact order. It uses a large set of computer-generated "hit and miss art" images. Cognitive validation needs a user to generate a path through a panel of images as follows: starting from the top-left corner image, moving down if the image is in their portfolio, or right otherwise. The user in needs to identify among steerer the row or column label that the path ends. This method was repeated, each time with a different panel. A successful login requires that the collective likelihood that corrects answers were not entered by a chance which exceeds a threshold within a given number of chances.

A ***recall*-based** system needs a user to regenerate the similar interaction result without cueing. Draw-A-Secret (DAS) was the first recall-based scheme proposed. A user needs to draw their password on a 2D grid. The system encrypts the sequence of grid cells along with the drawing path as a user drawn password this process will ahead up to successful login. Pass-Go enhances DAS's usability by encoding the grid intersection points quite than the grid cells. BDAS adds background images to DAS to encourage users to create more complex passwords.

ISSN: 2278 – 1323

In a ***cued-recall*** system, an exterior cue is provided to help for remembering and enter a password. Pass Points is a widely experienced click-based cued-recall system wherein a user needs to click a sequence of points anywhere on an image to creating a password, and to click the same order during the time of authentication. Cued Click Points (CCP) is similar to Pass Points but uses single image per click, then the next image selected by a deterministic function. Persuasive Cued Click Points (PCCP) extends CCP by requiring a user to choose a point inside a randomly positioned viewport when creating a password, follow-on in more randomly scattered click-points in a secret password.

In the midst of the above three types, recognition or acceptance technique is considered the easiest for human recollection in memory whereas pure recall is the hardest. Recognition system was typically the weakest level in resisting the online guessing attacks. Many proposed recognition-based schemes practically have a password space in the range of 2^14 to 2^16 passwords. A study states that a significant segment of passwords of DAS and Pass-Go were successfully broken with guessing attacks using dictionaries of 2^31to 2^42entries, as compared to the full password space of 2^58 entries. Images contain hotspots i.e., spots likely selected in creating passwords. Hotspots were exploited to ascend a successful guessing attacks on Pass Points a significant portion of passwords were broken with dictionaries of 2^26 to 2^34 entries, as compared and linked to the full space of 2^43passwords.

CAPTCHA:

The Captcha depends on the gap of capabilities between humans and bots in fixing certain hard AI problems. It contains two types of visual Captcha's (i.e.) text Captcha and Image-recognition Captcha (IRC). The previous relies on character recognition while the latter depends on recognition of non-character objects. Security of text Captcha's has been widely studied. The following Machine recognition of non-character objects is far less capable than character recognition. IRCs rely on the complexity of object identification or classification, perhaps combined with the difficulty of object segmentation. It mostly depends on binary object classification a user is asked to identify the bird from the panel of 12 images of flowers, birds and animals. Security of IRCs has also been studied (i.e.) captcha be capable of be circumvented through relay attacks whereby Captcha challenges are relayed to human solvers, whose answers are feed back to the targeted application.

CAPTCHA IN AUTHENTICATION:

This method was introduced in to use both Captcha and password in a user authentication protocol, which we will call as *Captcha-based Password Authentication (CbPA) protocol*, helps to defy the online dictionary attacks. The CbPA-protocol in order to solving a Captcha challenge after inputting a suitable pair of user ID and password unless a valid browser level cookie was received. For an invalid pair of user ID and password, the user has a certain level of probability to solve a Captcha challenge before being to deny their access. An Improved CbPA-protocol is wished-for to storing cookies only on the user-trusted machines and applying a Captcha challenge only when the number of failed login attempts for the specific account has exceeded a threshold limit. It is further improved in by applying a small threshold for failed login attempts from unknown machines but a large threshold for failed attempts from known machines with a previous successful login within a given period of time . Captcha was also used in recognition-based graphical passwords to address spyware and trojans, wherein a text Captcha is displayed below each image a user locates their own pass-images from distracted images, and enters the correct characters of each pass-image as their password during the time of authentication. Those specific locations were selected for each pass-image during password creation as a part of the password. In the above schemes of analyses, Captcha is an independent and individual entity, used together with a text, number as a graphical password. On the converse, a CaRP is both a Captcha and a graphical password technique.

IV. OVERVIEW OF CaRP

In the area of graphical passwords, Recognition based (pass faces) having high level of online guessing attacks. Recall based (draw a secret) shows high password strength but it needs very low level of attempts to crack the password. pccp is the latest technique which gives hot spot images (i.e.) highlighting the points to the attackers to crack it down. To overcome the existing system issues, the proposal system states about the end user having secured login authentication and validation scheme. It allows the user choice towards stronger and secured passwords than the conventional text passwords. In this system, text based captcha grid and image based captcha grid plays as a graphical passwords.Click text grid comprises of characters (i.e.) alphabets, numbers, special characters, in that grid confusing characters will be excluded like '0' & 'o' to avoid confusion. For click image, pools of image can be displayed, in that user need to choose their required passwords by done through enter via click based. So it resists the bots and online guessing attacks. By using hard AI problem, user can bypass the dictionary attacks; Xss(cross side scripting) doesn't work with the distorted images. By using dual view technology, it eradicates shoulder surfing attacks and relay attacks. It allows the user for secured and trustable authentication.

V. MODULE DESCRIPTION

5.1 CLICK TEXT GRID:

Click Text is a recognition-based CaRP scheme built on top of text Captcha grid. It contains alphabet comprise of characters without any visually-confusing. For example, Letter "O" and digit "0" may cause confusion in that image grid and so that characters should be excluded from the alphabet. A Click Text password is a sequence of characters in the alphabet, numbers, and special characters like e.g.,="A@B#9CD8$7". During generation, each character's position is tracked to produce a exact accuracy for the location of the character in the generated image (i.e). The characters should be trained and tested, and then only those characters will be binded on bitmap image. The

ISSN: 2278 – 1323

authentication server relies on the ground truth and hash values which stored at the time of user registration; it helps to identify the characters corresponding to user-clicked points at the time of user login. In Click Text images, characters can be arranged randomly on 2D space. This is different from normal type of text Captcha challenges.

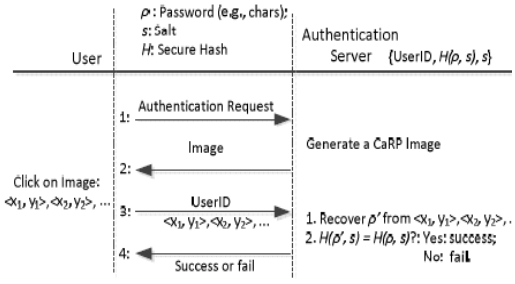
5.2 CLICK IMAGE GRID:

Click image is a recognition-based CaRP scheme built on top of Captcha-image pool grid, like an alphabets of click text, similarly images can be arranged such as flowers, pets, etc. The Captcha generation process is applied to generate Click images on grid, the user need to choose their image password in 2D images by applying different shapes, textures, colors, effects, and optionally distortions of selected image. The resulting 2D images are then arranged and binded on a cluttered background such as grassland. Note that different views applied to 2D images which the user selected as a password. Then take the coordinate values of that chosen image in that bitmap image grid. Combined with the additional anti-recognition mechanisms

5.3 IMAGE WITH NUMBER GRID:

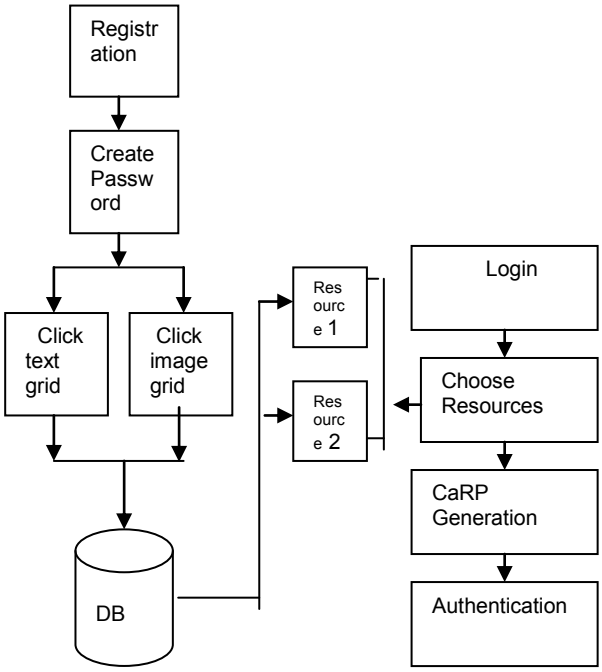
Applied in the mapping step, these make it hard for computers to automatically recognize images in the generated image pool, but humans as a user can easily identify different instantiations of images. CaRP should have a sufficiently-large effective password space to resist human guessing attacks. Image grid is a combination of Click image and CAS (click a secret)(i.e.)Images behind a number grid. To enter a password, a Click image is displayed first. After an Image is selected, an image of n× n grid appears, with the grid-cell size which equals the bounding rectangle of the selected image. Each grid-cell is labeled to help users to identify. Once the bounding rectangle of the selected image is identified, an image of n× n number grid with the identified bounding rectangle as its grid-cell size is generated and displayed. If the grid image is too big or too little for a user to view, then the grid image is adjusted to a apt size. Then the user will click the respective same image from the backdrop grid the above process is repeated until the user has finished entering their password. The resulting sequence of coordinates of user clicked points, e.g., "IP<150,55>, GP<35,66>, …" where "IP<x,y>" denotes the point with coordinates <x , y> on a Click image, and "GP<x , y>" denotes the point with coordinates <x , y> on a grid image, is sent to the authentication server with a hash values.

5.4 AUTHENTICATION USING CARP SCHEME:



Here that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server. The authentication server (AS) stores a salt (s) and a hash value H (P, S) for each user ID by MD5 algorithm, where the password of the account is are not stored only hash values. A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects at the time of registration, (AS) generates a CaRP image and records the locations of the objects in the image. Then the time of authentication that the user needs to clicked on the image. Then (AS) retrieves salt (S) of the account, calculates the hash value of (P) and compare with the salt, and then match the obtained result with the hash value which is already stored for that account. Validation succeeds only if the two hash values get matched. This series of process is called the basic CaRP level authentication.

VI. SOLUTION ARCHITECTURE:



The solution architecture diagram states about the overall idea of the project, it makes us to understand how it flows from starting to end phase, in this project solution architecture diagram representation clearly about registration and two types of login phase , through that how user can authenticated securely can be explained in detail.

VII. CONCULSION

This paper states about CaRP, a new security primitive depends on unsolved hard AI problems. CaRP is a combination of both Captcha and a graphical password system. The view of CaRP introduces a new idea of graphical passwords, which acquired a new level of approach to defy mainly online guessing attacks a new raise of CaRP image, which is also, seems like a Captcha challenge, it is used for every login challenge to make trials of an online guessing attack computationally autonomous of each other. A password of CaRP can be found in a probabilistic way of automatic online guessing attacks,

ISSN: 2278 – 1323

including of brute-force attack too. Hotspots in CaRP images can be no longer be exploited to initiate automatic online guessing attacks, which is an innate weakness in many graphical password systems. CaRP forces adversary to way out to significantly less efficient and much more costly in human-based attacks. It also offers protection from online guessing attacks, CaRP is also defiant to Captcha relay attacks, cross-site scripting attacks, and, if joined with dual-view technologies, it sort out shoulder-surfing attacks. CaRP will help to reduce spam emails send from a Web email service. As a framework, CaRP does not depend on any specific Captcha system. When any one Captcha scheme is broken, a new & more secure levels may appear and to be converted as a CaRP scheme. On the whole, our effort in this work is one step forward and advances in the idea of using hard AI problems for security enhancements. It supports up to a level of reasonable security and usability to practical applications, the CaRP has good potential level for refinements, which will be entitle for functional future enhancement work. More essentially, we will be expecting a CaRP to inspire new inventions of such AI based security primitives.

REFERENCES

1. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N.Memon, "PassPoints: design and longitudinal evaluation of agraphical password system," *Int. Journal of HCI,* vol. 63,2005, pp. 102–127.

2. Real User Corporation. *The science behind Passfaces*. White paper, http://www.realuser.com/published/ ScienceBehindPassfaces.pdf, accessed Feb. 2012.

3. I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *8th USENIX Security Symposium*, 1999.

4. H. Tao and C. Adams, "Pass-Go: A proposal to improve theusability of graphical passwords," *Int. Journal of NetworkSecurity*, vol. 7, no.

5. P. C. van Oorschot and S. Stubblebine, "On countering online dictionary attacks with login histories and humans-inthe- loop," *ACM Trans. Info. System Security*, vol. 9, no. 3,2006, pp. 235-258.

6. L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "Captcha: Using hard AI problems for security," in *Eurocrypt*, 2003, pp. 294-311.

7. S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *European Symposium on Research in Computer Security (ESORICS),* 2007, pp. 359-374.

8. S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: persuasive cued click-points, in *Proc. British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction*, vol. 1, 2008, pp. 121-130.

Authors :

1. Name: A.RAGAVENDRA, acknowledged the B.Tech degree in Computer Science and Engineering from Anna University of Chennai, Currently pursuing M.Tech in Information Security and Cyber Forensics at SRM University, Kattankulathur, Chennai, Tamilnadu, India

2. Name: Mrs.J.JEYSREE Working as an Assistant Professor, department of Information Technology at SRM University, Kattankulathur, Chennai, Tamilnadu, India.

ISSN: 2278 – 1323